Cryptosystems from supersingular elliptic curve isogenies

Presented by
Nicola Dal Cin ist1104444

Instituto Superior Técnico

TÉCNICO LISBOA

TOWARDS QUANTUM-RESISTANT CRYPTOSYSTEMS FROM SUPERSINGULAR ELLIPTIC CURVE ISOGENIES

LUCA DE FEO, DAVID JAO, AND JÉRÔME PLÛT

ABSTRACT. We present new candidates for quantum-resistant public-key cryptosystems based on the conjectured difficulty of finding isogenies between supersingular elliptic curves. The main technical idea in our scheme is that we transmit the images of torsion bases under the isogeny in order to allow the parties to construct a shared commutative square despite the noncommutativity of the endomorphism ring. Our work is motivated by the recent development of a subexponential-time quantum algorithm for constructing isogenies between ordinary elliptic curves. In the supersingular case, by contrast, the fastest known quantum attack remains exponential, since the noncommutativity of the endomorphism ring means that the approach used in the ordinary case does not apply. We give a precise formulation of the necessary computational assumptions along with a discussion of their validity, and prove the security of our protocols under these assumptions. In addition, we present implementation results showing that our protocols are multiple orders of magnitude faster than previous isogeny-based cryptosystems over ordinary curves.

This paper is an extended version of [19]. We add a new zero-knowledge identification scheme, and detailed security proofs for the protocols. We also present a new, asymptotically faster, algorithm for key generation, a thorough study of its optimization, and new experimental data.

Keywords: elliptic curves, isogenies, quantum-resistant public-key cryptosystems

- Public–key cryptosystem based on supersingular curves
  - Zero–knowledge proof of identity
  - Key exchange
  - Public–key encription

TÉCNICO LISBOA

1. *Minima* on elliptic curves
   - Group structure
   - Isogenies
   - Supersingular elliptic curves
2. Cryptosystem
   - Zero–knowledge proof of identity
   - Key exchange
   - Public–key encryption
3. Security and complexity
   - Computing isogenies
   - Security

Minima on elliptic curves

TÉCNICO LISBOA

Definition

An **elliptic curve** E over a field k is a smooth *projective curve* (defined on k) with genus 1 and a distinguished k–rational point.

- The crucial property of elliptic curves is that is possible to define an **(abelian) group structure** on the rational points $E(k)$.
- Indeed, elliptic curves are **abelian varieties** [2].
- The group law that one defines is indeed algebraic!

TÉCNICO LISBOA

Definition

An **elliptic curve** E over a field k is a smooth *projective curve* (defined on k) with genus 1 and a distinguished k–rational point.

- The crucial property of elliptic curves is that is possible to define an **(abelian) group structure** on the rational points $E(k)$.
- Indeed, elliptic curves are **abelian varieties** [2].
- The group law that one defines is indeed algebraic!

TÉCNICO LISBOA

Definition

An **elliptic curve** E over a field k is a smooth *projective curve* (defined on k) with genus 1 and a distinguished k–rational point.

- The crucial property of elliptic curves is that is possible to define an **(abelian) group structure** on the rational points $E(k)$.
- Indeed, elliptic curves are **abelian varieties** [2].
- The group law that one defines is indeed algebraic!

TÉCNICO LISBOA

Definition

An **elliptic curve** E over a field k is a smooth *projective curve* (defined on k) with genus 1 and a distinguished k–rational point.

- The crucial property of elliptic curves is that is possible to define an **(abelian) group structure** on the rational points $E(k)$.
- Indeed, elliptic curves are **abelian varieties** [2].
- The group law that one defines is indeed algebraic!

TÉCNICO LISBOA

Theorem

Up to isomorphism, **every** elliptic curve over k (with $char(k) \neq 2, 3$) can be determined by an affine equation of the form

$$y^2 = x^3 + Ax + B, \tag{1}$$

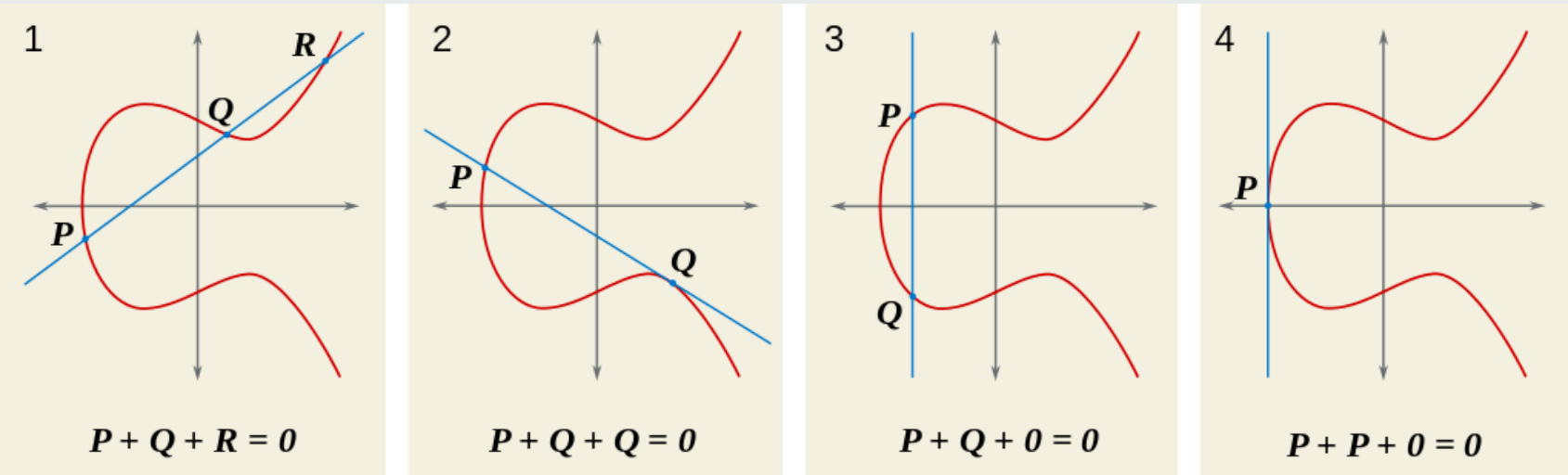
where $A, B \in k$ and $4A^3 + 27B^2 \neq 0$.

Theorem (Bezout)

Let E be an elliptic curve on k; then every line in $P^2(\bar{k})$ cuts its Weierstrass curve in exactly three points (counted with multiplicity).

The previous characterization and Bezout's theorem lead to a natural way to define the group law:

$$P + Q + R \stackrel{def}{=} O. \tag{2}$$



TÉCNICO LISBOA

Definition

Consider an elliptic curve E/k defined by

$$E : y^2 = x^3 + Ax + B, \quad A, B \in k.$$

The quantity

$$j = 1728 \frac{4A^3}{4A^3 + 27B^2}$$

is called the **j-invariant** of E.

Theorem (Mordell 1922)

The group $E(\mathbb{Q})$ is a finitely generated abelian group. Thus

$$E(\mathbb{Q}) \simeq T \oplus \mathbb{Z}^r, \tag{3}$$

where the **torsion subgroup T** is a finite abelian group corresponding to the elements of $E(\mathbb{Q})$ with finite order, while r is the **rank** of $E(\mathbb{Q})$.

TÉCNICO LISBOA

Theorem (Hasse 1933)

The cardinality of $E(\mathbb{F}_p)$ on average is $p+1$; more precisely

$$\#E(\mathbb{F}_p) = p + 1 - t, \quad \text{with} \quad |t| \leq 2\sqrt{p}. \tag{4}$$

TÉCNICO LISBOA

Definition

An isogeny is an algebraic morphism ϕ between elliptic curves (on K) that preserves the point at infinity.

- What is important in our framework is that an isogeny can be expressed as a pair of rational functions:

$$\phi(x, y) = \left(\frac{p(x, y)}{q(x, y)}, \frac{r(x, y)}{s(x, y)} \right), \quad \text{with } p, r, q, s \in K[x, y].$$

TÉCNICO LISBOA

Definition

An isogeny is an algebraic morphism ϕ between elliptic curves (on K) that preserves the point at infinity.

- What is important in our framework is that an isogeny can be expressed as a pair of rational functions:

$$\phi(x,y) = \left(\frac{p(x,y)}{q(x,y)}, \frac{r(x,y)}{s(x,y)}\right), \quad \text{with } p,r,q,s \in K[x,y].$$

The **multiplication by m** is the map defined as $P \mapsto [m]P = P + \cdots + P$.

Definition

The **m-torsion subgroup** of a curve E is

$$E[m] := \{P \in E(\overline{K}) : [m]P = \mathcal{O}\}.$$

TÉCNICO LISBOA

Definition

An elliptic curve E/k, where char $k = p$, such that

$$E[p^r] = 0, \quad \text{for all } r \geq 1,$$

is said a **supersingular elliptic curve.**

Cryptosystem

Cryptosystem definition

"Ingredients"

- Fix $\mathbb{F}_q = \mathbb{F}_{p^2}$ with $p = \ell_A^{e_A} \ell_B^{e_B} \cdot f \pm 1$ a prime.
- Construct a supersingular curve $E/\mathbb{F}_{p^2}$ with (smooth) cardinality $(\ell_A^{e_A} \ell_B^{e_B} \cdot f)^2$.
- By construction $E[\ell_A^{e_A}]$ contains $\ell_A^{e_a - 1}(\ell_A + 1)$ cyclic subgroups of order $\ell_A^{e_A}$ each defining a different isogeny.

Cryptosystem definition

"Ingredients"

- Fix $\mathbb{F}_q = \mathbb{F}_{p^2}$ with $p = \ell_A^{e_A} \ell_B^{e_B} \cdot f \pm 1$ a prime.
- Construct a supersingular curve $E/\mathbb{F}_{p^2}$ with (smooth) cardinality $(\ell_A^{e_A} \ell_B^{e_B} \cdot f)^2$.
- By construction $E[\ell_A^{e_A}]$ contains $\ell_A^{e_a - 1}(\ell_A + 1)$ cyclic subgroups of order $\ell_A^{e_A}$ each defining a different isogeny.

- Fix $\mathbb{F}_q = \mathbb{F}_{p^2}$ with $p = \ell_A^{e_A} \ell_B^{e_B} \cdot f \pm 1$ a prime.
- Construct a supersingular curve $E/\mathbb{F}_{p^2}$ with (smooth) cardinality $(\ell_A^{e_A} \ell_B^{e_B} \cdot f)^2$.
- By construction $E[\ell_A^{e_A}]$ contains $\ell_A^{e_a - 1}(\ell_A + 1)$ cyclic subgroups of order $\ell_A^{e_A}$ each defining a different isogeny.

- Peggy knows a cyclic degree $\ell_A^{e_A}$ isogeny $\phi : E \to E/\langle S \rangle$ and wants to prove Vic that she knows a generator for $\langle S \rangle$.
- At each iteration she takes a random $\langle R \rangle$ cyclic group of order $\ell_B^{e_B}$ and computes the diagram:

$$\begin{array}{ccc} E & \xrightarrow{\phi} & E/\langle S \rangle \\ \downarrow{\scriptstyle \psi} & & \downarrow{\scriptstyle \psi'} \\ E/\langle R \rangle & \xrightarrow{\phi'} & E/\langle S, R \rangle \end{array}$$

Theorem

Let E/K be an elliptic curve and $G < E$ a finite subgroup. Then, there is a **unique** curve (up to isomorphism) E' and a **separable** isogeny ϕ such that

$$\phi : E \to E' =: E/G, \quad \ker \phi = E'. \tag{5}$$

Given a subgroup, it is possible to construct the correspondent isogeny.

- Suppose E/K is $y^2 = x^3 + ax + b$ and $\#G = l$ an odd prime.
- For a $Q = (x_Q, y_Q) \in G^*$, define

$$t_Q = 3x_Q^2 + a, \quad u_Q = 2y_Q^2, \quad w_Q = u_Q + t_Q x_Q$$

$$t = \sum_{Q \in G^*} t_Q, \quad w = \sum_{Q \in G^*} w_Q \quad \text{and} \quad r(x) = x + \sum_{Q \in G^*} \left(\frac{t_Q}{x - x_Q} + \frac{u_Q}{(x - x_Q)^2} \right).$$

- The isogeny ϕ and its image $\phi(E) = E/K$ are then

$$\phi = (r(x), r'(x)y) \quad \text{and} \quad \phi(E) : y^2 = x^3 + (a - 5t)x + (b - 7w).$$

Given a subgroup, it is possible to construct the correspondent isogeny.

- Suppose E/K is $y^2 = x^3 + ax + b$ and $\#G = l$ an odd prime.
- For a $Q = (x_Q, y_Q) \in G^*$, define

$$t_Q = 3x_Q^2 + a, \quad u_Q = 2y_Q^2, \quad w_Q = u_Q + t_Q x_Q$$

$$t = \sum_{Q \in G^*} t_Q, \quad w = \sum_{Q \in G^*} w_Q \quad \text{and} \quad r(x) = x + \sum_{Q \in G^*} \left(\frac{t_Q}{x - x_Q} + \frac{u_Q}{(x - x_Q)^2} \right).$$

- The isogeny ϕ and its image $\phi(E) = E/K$ are then

$$\phi = (r(x), r'(x)y) \quad \text{and} \quad \phi(E) : y^2 = x^3 + (a - 5t)x + (b - 7w).$$

Given a subgroup, it is possible to construct the correspondent isogeny.

- Suppose E/K is $y^2 = x^3 + ax + b$ and $\#G = l$ an odd prime.
- For a $Q = (x_Q, y_Q) \in G^*$, define

$$t_Q = 3x_Q^2 + a, \quad u_Q = 2y_Q^2, \quad w_Q = u_Q + t_Q x_Q$$

$$t = \sum_{Q \in G^*} t_Q, \quad w = \sum_{Q \in G^*} w_Q \quad \text{and} \quad r(x) = x + \sum_{Q \in G^*} \left(\frac{t_Q}{x - x_Q} + \frac{u_Q}{(x - x_Q)^2} \right).$$

- The isogeny ϕ and its image $\phi(E) = E/K$ are then

$$\phi = (r(x), r'(x)y) \quad \text{and} \quad \phi(E) : y^2 = x^3 + (a - 5t)x + (b - 7w).$$

Zero–knowledge proof of identity

Secret parameters: A supersingular curve E defined over $\mathbb{F}_q$ and a primitive $\ell_A^{e_A}$-torsion point S defining an isogeny $\phi : E \to E/\langle S \rangle$.
Public parameters: The curves E and $E/\langle S \rangle$. Generators P, Q of $E[\ell_B^{e_B}]$ and their images $\phi(P), \phi(Q)$.
Identification: Repeat m times:

(1) Peggy chooses a random primitive $\ell_B^{e_B}$-torsion point R and computes diagram (3).
(2) Peggy sends the curves $E_1 = E/\langle R \rangle$ and $E_2 = E/\langle S, R \rangle$ to Vic.
(3) Vic selects a random bit b and sends it to Peggy.
(4) If $b = 0$, Peggy reveals the points R and $\phi(R')$. Vic accepts if they have order $\ell_b^{e_B}$ and generate the kernels of isogenies $E \to E_1$ and $E/\langle S \rangle \to E_2$, respectively.
(5) If $b = 1$, Peggy reveals the point $\psi(S)$. Vic accepts if it has order $\ell_A^{e_A}$ and generates the kernel of an isogeny $E_1 \to E_2$.

Figure: ZN protocol

Key exchange

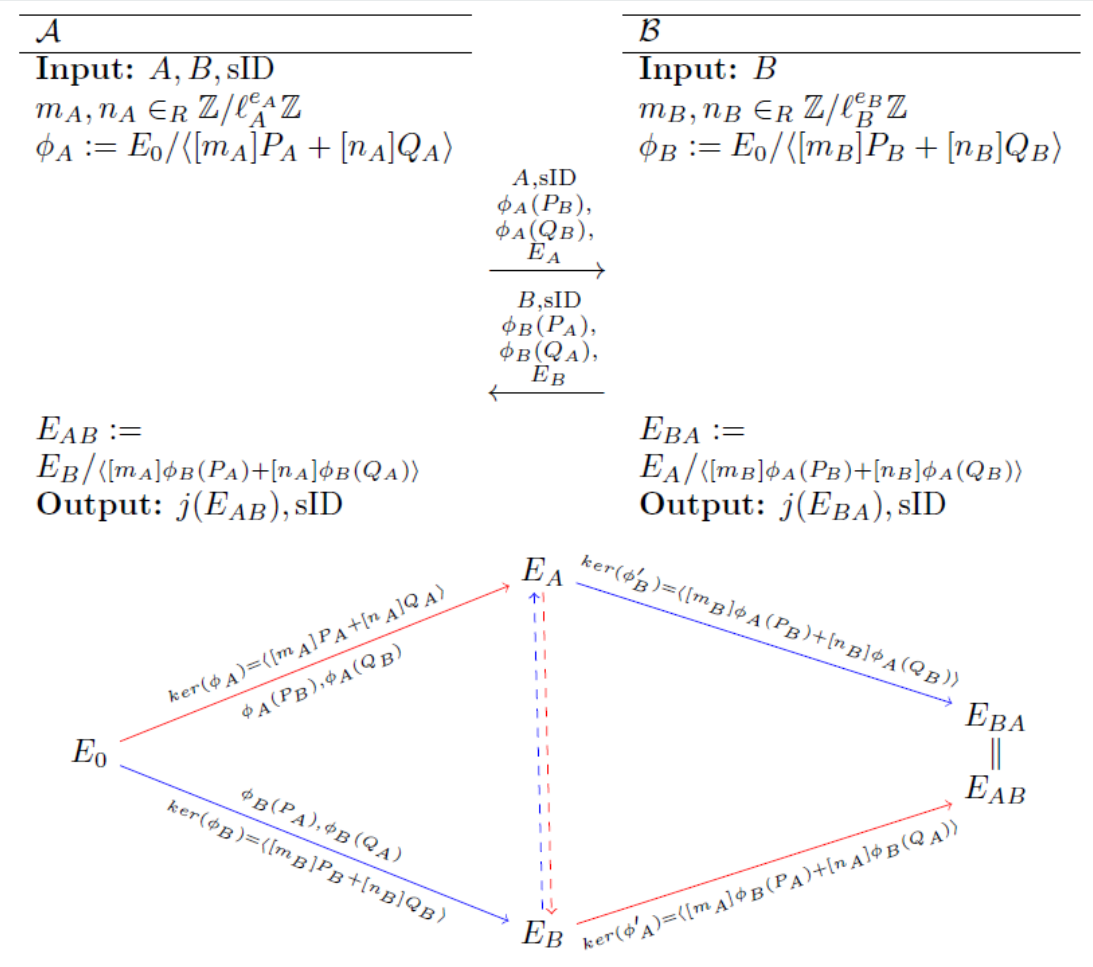


Figure: Key exchange protocol.

Setup: Choose $p = \ell_A^{e_A} \ell_B^{e_B} \cdot f \pm 1$, E_0, $\{P_A, Q_A\}$ and $\{P_B, Q_B\}$ as before. Let $\mathcal{H}$ a hash function family with indexes in a finite set K, i.e.

$$H_k : \mathbb{F}_{p^2} \to \{0,1\}^\omega, \quad \forall k \in K.$$

Key generation: Choose $m_A, n_A \in_R \mathbb{Z}/\ell_A^{e_A}\mathbb{Z}$ not both divisible by ℓ_A. Then

Public key = $(E_A, \phi_A(P_B), \phi_A(Q_B), k)$, with $k \in_R K$,

Private key = (m_A, n_A, k).

Encryption: Given a public key $(E_A, \phi_A(P_B), \phi_A(Q_B), k)$ and a message $m \in \{0,1\}^\omega$, choose $m_B, n_B \in_R \mathbb{Z}/\ell_A^{e_B}\mathbb{Z}$ and compute

$$h = H_k(j(E_{AB})), \quad c = h \oplus m.$$

Cyphertext = $(E_B, \phi_B(P_A), \phi_B(Q_A), c)$.

Decryption: Given a cyphertext $(E_B, \phi_B(P_A), \phi_B(Q_A), c)$ and a private key (m_A, n_A, k), compute the j-invariant $j(E_{AB})$ and set

$$h = H_k(j(E_{AB})), \quad m = h \oplus c.$$

Plaintext = m.

Security and complexity

How Alice and Bob can compute and evaluate an isogeny $\phi : E \to E/\langle R \rangle$?

- Since deg $\phi = \ell^e$ is smooth we can write a chain of ℓ-isogenies:

$$\phi = \phi_{e-1} \circ \cdots \circ \phi_0,$$

where $E_0 := E$, $R_0 := R$, and

$$\phi_i : E_i \to E_{i+1} := E_i/\langle \ell^{e-i-1} R_i \rangle$$

with $R_{i+1} := \phi_i(R_i)$.

- This suggested a strategy with quadratic complexity in e.

How Alice and Bob can compute and evaluate an isogeny $\phi : E \to E/\langle R \rangle$?

- Since deg $\phi = \ell^e$ is smooth we can write a chain of ℓ-isogenies:

$$\phi = \phi_{e-1} \circ \cdots \circ \phi_0,$$

where $E_0 := E$, $R_0 := R$, and

$$\phi_i : E_i \to E_{i+1} := E_i/\langle \ell^{e-i-1} R_i \rangle$$

with $R_{i+1} := \phi_i(R_i)$.

- This suggested a strategy with quadratic complexity in e.

How Alice and Bob can compute and evaluate an isogeny $\phi : E \to E/\langle R \rangle$?

- Since deg $\phi = \ell^e$ is smooth we can write a chain of ℓ-isogenies:

  $$\phi = \phi_{e-1} \circ \cdots \circ \phi_0,$$

  where $E_0 := E$, $R_0 := R$, and

  $$\phi_i : E_i \to E_{i+1} := E_i/\langle \ell^{e-i-1} R_i \rangle$$

  with $R_{i+1} := \phi_i(R_i)$.

- This suggested a strategy with quadratic complexity in e.

Isogeny graphs

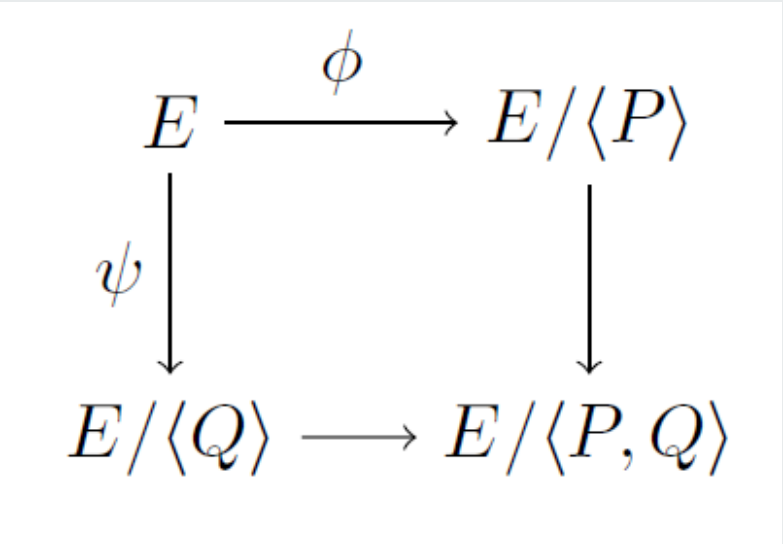
TÉCNICO LISBOA

Definition

An ℓ-**isogeny graph** $\mathcal{G}_\ell$ is a graph that has elliptic curves over $\mathbb{F}_q$ (up to isomorphism) as vertices. Two nodes E and E' are connected if there exists an ℓ-degree isogeny from E to E'.

If we consider only supersingular elliptic curves

- there is a finite number ($\approx p/12$) of isomorphism classes, i.e. of vertices.
- All supersingular elliptic curves belong to the same isogeny class, i.e. the graph is connected.
- In an isogeny graph of elliptic curves a random walk quickly reach an (almost) uniform distribution over the vertices.



Our protocol is based on this commutative diagram, where ϕ and ψ are essentially random walks in the graphs of isogenies of degree ℓ_A and ℓ_B.

- The hardness of finding a path connecting two verteces in a graph of supersingular isogenies is the core of SIDH security.

References I

[1] L. De Feo, D. Jao, and J. Plût, “Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies,” *Journal of Mathematical Cryptology*, vol. 8, no. 3, pp. 209–247, 2014.

[2] J. H. Silverman, *The arithmetic of elliptic curves*, vol. 106. Springer, 2009.